

ECS Configuration Change Request

Page 1 of

Page(s)

1. Originator Henry Baez	2. Log Date: 1 AUG 00	3. CCR #: 00-0790	4. Rev: —	5. Tel: 925-1025	6. Rm #: 2101D	7. Dept. SED
8. CCR Title: Install Hewlett-Packard provided ftpd binary to replace current HP ftpd binary that has several security vulnerability.						
9. Originator Signature/Date <i>Henry Baez</i> 7/28/2000		10. Class II	11. Type: CCR	12. Need Date: 8-1-2000		
13. Office Manager Signature/Date <i>Randy Haynes</i> 7/28/00		14. Category of Change: Initial ECS Baseline Doc.		15. Priority: (If "Emergency" fill in Block 28). Routine EMERGENCY		
16. Documentation/Drawings Impacted: <i>N/A</i>		17. Schedule Impact:		18. CI(s) Affected:		
19. Release Affected by this Change: 5A		20. Date due to Customer:		21. Estimated Cost: None - Under 100K		
22. Source Reference: <input type="checkbox"/> NCR (attach) <input type="checkbox"/> Action Item <input checked="" type="checkbox"/> Tech Ref. <input type="checkbox"/> GSFC <input type="checkbox"/> Other: Hewlett-Packard Company Security Advisory: #00117, 11 July '00						
23. Problem: (use additional Sheets if necessary) There are 2 problems with FTP Server (ftpd) on HP-UX. First ftpd handling of the SITE EXEC command that allows remote users to gain root access. This is possible in the default configuration of ftpd on HP-UX 11.00 ONLY. Second, ftpd does not properly format the parameters to the setproctitle() function, allowing users to gain root access. This problem applies to both HP-UX 11.00 and 10.X.						
24. Proposed Solution: (use additional sheets if necessary) Install in /usr/sbin the new binary ftpd, with permissions 544, the correct temporary binary for the version of HP-UX baseline, 10.2. The binary and procedure has been tested at the GDAAC. Both cksum and MD5 signature have been check on download binary. <i>FILE IS CALLED ftpd31-07-00 IS LOCATED IN /data/CM-IVBOX. CKSUM 3969082595, MD5 90112</i>						
25. Alternate Solution: (use additional sheets if necessary) Turn off FTP services for all HP-UX platforms.						
26. Consequences if Change(s) are not approved: (use additional sheets if necessary) If the new ftpd binary is not used and the vulnerable ftpd is kept in service, there is the possibility that this vulnerability could be exploited to gain root access and create disruptions and down time of EOS systems.						
27. Justification for Emergency (If Block 15 is "Emergency"): <i>THERE IS AN HP AT EACH DAAL THAT IS ON THE USER LAN AND THEREFORE VULNERABLE TO CRACKERS ON THE INTERNET</i>						
28. Site(s) Affected: <input checked="" type="checkbox"/> EDF <input checked="" type="checkbox"/> PVC <input checked="" type="checkbox"/> VATC <input checked="" type="checkbox"/> EDC <input checked="" type="checkbox"/> GSFC <input checked="" type="checkbox"/> LaRC <input checked="" type="checkbox"/> NSIDC <input checked="" type="checkbox"/> SMC <input type="checkbox"/> AK <input type="checkbox"/> JPL <input type="checkbox"/> EOC <input type="checkbox"/> IDG Test Cell <input type="checkbox"/> Other						
29. Board Comments:			30. Work Assigned To:		31. CCR Closed Date:	
32. EDF/SCDV CCB Chair (Sign/Date): <i>Bryan V. Vitar</i> 8/1/00		Disposition: <u>Approved</u> App/Com. Disapproved Withdraw Fwd/ESDIS ERB				
33. M&O CCB Chair (Sign/Date): <i>W. B. ...</i> 8/1/00		Disposition: <u>Approved</u> App/Com. Disapproved Withdraw Fwd/ESDIS Fwd/ECS				
34. ECS CCB Chair (Sign/Date):		Disposition: <u>Approved</u> App/Com. Disapproved Withdraw Fwd/ESDIS ERB				

CM01JA00

ECS/EDF/SCDV/M&O

ORIGINAL